Information Security Risk Management

Handbook for ISO/IEC 27001

Edward Humphreys

First published in the UK in 2010

by
BSI
389 Chiswick High Road
London W4 4AL

Typeset in Caslon Pro and Franklin Gothic by Monolith – http://www.monolith.uk.com
Printed in Great Britain by Berforts, www.berforts.co.uk

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978-0-580-60745-5

Contents

This book is dedicated to my father, Thomas Edward Humphreys, and my mother, Alice Theresa (Stewart) Humphreys, and also to my sons Alexander, Thomas and James, and of course Anji.

I would like to thank all those reviewers, Dale Johnstone, Dr Angelika Plate, Dick Price and John Snare for their suggestions and invaluable comments.

Edward Humphreys

1 Introduction

1.1 Importance of risk management

Organizations, governments, society and citizens face many threats and risks. No one in these four broad groups is excluded from the situation. In addition we, as individuals, are both risk takers and risk averse depending on the particular circumstances we are in. We may take risks in one area of our lives and be risk averse in another area.

Modern society is highly dependent on the use of IT for commercial and private use. IT presents us with a variety of risks. As individuals we take risks and we are at risk: what we do, how we do things, and how we interact with the IT we use and the environment in which we live and work. There are also specific categories of risk – for example, physical and environmental risks, safety risks, health risks, financial risks, operational risks and, of course, information security risks.

Information is a business asset with varying levels of commercial value and sensitivity. In addition, some of this information is personal data. This means that information needs to be protected from the risk of being stolen, misused, modified, destroyed, or not being available to those authorized to have use of such information.

Information security is now a mainstream political, economic, societal and business issue. It is no longer the province of technologists alone; it is a far broader issue affecting all from the CEO, the company board, shareholders, senior and middle management through to every user and member of staff in the organization, irrespective of rank or job role.

1.2 Risk focused strategy

To be meaningful to the organization, a strategy for dealing with information security risks must be considered in a business context, and the interrelationships with other business functions – such as human resources, research and development, production and operations, administration, IT, finance and customers – need to be identified, to achieve a holistic and complete picture of these risks. This should include taking account of the organizational risks, and applying the concepts and

ideas of corporate governance. This, together with the organization's business, effectiveness and the legal and regulatory environment, all serve as drivers and motivators for a successful risk management process. These ideas are explored in more detail in Chapter 3.

This book is focused on the concept of having an information security management system (ISMS) as the framework for achieving the effective management of information security risks. The international standard ISO/IEC 27001 is the world-recognized standard for establishing, implementing, monitoring and reviewing, updating and improving an ISMS.

This book is aimed at those business managers and their staff involved in ISMS risk management activities as a practical handbook for ISO/IEC 27005:2009 and ISO/IEC 27001:2005. It provides guidance and advice specifically to support the implementation of those requirements defined in ISO/IEC 27001:2005 that relate to risk management processes and associated activities. Many of the definitions used in this book are aligned with the generic risk standard ISO 31000:2009.

These ISO/IEC standards have adopted the process approach for assessing and treating risks, ongoing risk monitoring, risk reviews and reassessments. A process approach encourages users to take into account the importance of:

- understanding business information security requirements and the need to establish policy and objectives for information security;
- selecting, implementing and operating controls in the context of managing an organization's overall business risks;
- monitoring and reviewing the performance and effectiveness of the ISMS to manage the business risks;
- continual improvement based on objective risk measurement.

1.3 Risk process

This risk management process focuses on providing the business with an understanding of risks to allow effective decision-making to be applied to control the risks. The risk management process is an ongoing activity that aims to continuously improve the efficiency and effectiveness of the organization's ISMS implementation.

The risk management process should be applied to the whole ISMS (as specified in ISO/IEC 27001:2005) – that is, all elements of the ISMS. The process needs to be applied at the planning and design stages as well as the subsequent stages of operational deployment, monitoring and review of the risks, and the updating and improvement stages to ensure that any information security risks are always being appropriately managed.

An important part of the risk management process is the assessment of information security risks. This is necessary to understand the business information security requirements, and the risks to the organization's business assets. In ISO/IEC 27001:2005, the risk assessment includes the following actions and activities, which are described in more detail in Chapter 4:

- identification of assets;
- identification of legal and business requirements that are relevant for the identified assets;
- valuation of the identified assets, taking account of the identified legal and business requirements and the impacts of a loss of confidentiality, integrity and availability;
- identification of significant threats to, and vulnerabilities of, the identified assets;
- assessment of the likelihood of the threats and vulnerabilities to occur;
- calculation of risk;
- evaluation of the risks against a predefined risk scale.

The next step in the risk management process is to identify the appropriate actions to be taken for the treatment of each of the risks that have been identified during the risk assessment. Risks can be managed through a combination of prevention and detection controls, avoidance tactics, insurance and/or simple acceptance. Once a risk has been assessed, a business decision needs to be made on what, if any, action should be taken. In all cases, the decision should be based on a business case which justifies the decision and which can be accepted or challenged by key stakeholders. The different risk treatment options and factors that influence this decision are described in Chapter 5.

Once the risk treatment decisions have been made and the controls that were selected following these decisions have been implemented, the ongoing risk management activities should start. These activities include the process of monitoring the risks and the performance of the ISMS to ensure that the implemented controls work as intended. A further activity is risk review and reassessment, which is necessary to adapt the risk assessment to the changes that may occur over time in the business environment. Risk reporting and communication is necessary to ensure that business decisions are taken in the context of an organization-wide understanding of risks. The co-ordination of the different risk-related processes should ensure that the organization can operate in an efficient and effective way. Continual improvement is an essential part of the ongoing risk management activities to increase the effectiveness of the implemented controls towards achieving the goals that have been set for the ISMS. The ongoing risk management activities are described in Chapter 7.

The successful implementation of the risk management process requires that roles and responsibilities are clearly defined and discharged within the organization. Roles and responsibilities that are involved in the risk management process are included in ISO/IEC 27005, as relevant.

This Handbook gives guidance to support the requirements given in ISO/IEC 27001:2005 and the advice given in ISO/IEC 27005, regarding all aspects of an ISMS risk management cycle. This cycle includes assessing and evaluating the risks, implementing controls to treat the risks, monitoring and reviewing the risks, and maintaining and improving the system of risk controls.

1.4 Target audience

This Handbook is intended to be applicable to all organizations, regardless of their type, size and nature of business. It is intended for those business managers and their staff involved in ISMS risk management activities. It would also be useful for training and educational purposes and to anyone with an interest in the risk management aspects of ISO/IEC 27001:2005.

2 Nature of the Information Security Risk Landscape

2.1 Risk – what is it?

2.1.1 Definitions

Giving a definition of risk is difficult given the wide variety of ways in which the term is used and applied to different fields and applications. What is generally common to these different uses is that the context usually considers:

- uncertainty; and
- undesirable consequences.

For the purposes of interpreting the term 'information security risk' as it is used in this book we shall use the following definition:

> **Risk** = combination of the risk of exposure and the impact = combination of (likelihood of the threat being able to expose an element(s) of the system) and impact
>
> **Risk of exposure** is the likelihood that an element of the system lacks enough protection to be able to counter the effects of a threat. In other words, there is a likelihood that the system element is exposed to being at risk.

The *uncertainty* is that the organization can only estimate how likely it is to experience the risk of exposure; it cannot work on a basis of certainty. The *undesirable consequence* is the impact to which the organization may be subjected if its assets are exposed to risks. Here we have an important link between the impact and the value of the assets at risk.

The 'likelihood' is used to obtain estimates based on unknown parameters and on known outcomes. Therefore, in the risk definition above it is the 'likelihood' that the threats (unknown parameters) might be able to exploit weaknesses in

the organization, to cause a risk of exposure. Sometimes the word 'probability' is used as a synonym for 'likelihood', particularly in non-technical everyday speech. However, there are technical and mathematical differences between 'likelihood' and 'probability': 'probability' allows us to predict unknown outcomes based on known parameters whereas 'likelihood' is based on unknown parameters and on known outcomes.

CASE STUDY EXAMPLES

1. Asset = **Company sensitive information on future investments**

This information is likely to be extremely valuable for the future of the company. Therefore, if it were to be lost, stolen or severely damaged in any way, the impact might be devastating for the future of the company, its financial state, its position in the market and its market shares and profits.

2. Asset = **Customer personal data**

This information is likely to be extremely important to the customers and might also be very sensitive. Therefore, if it were to be lost, stolen or severely damaged in any way, the impact might be devastating for both customers and the company. The company could suffer legal action, damage to its reputation and loss of customer confidence leading to customers taking their business elsewhere to a competitor. Similarly, to the customer there may be several impacts including financial loss as well as personal damage to the individual's standing, image and so on.

3. Asset = **Company funds**

These funds are of financial importance to the organization; therefore, if these funds were to be stolen through fraudulent activities, this would have a direct impact on company finances and might involve legal or regulatory action.

2.1.2 A world of risk

We live and work in a world in which society and the environment around us is inherently at risk. Nothing is certain in life and as a society we need to live with this fact. We cannot afford to be complacent and take the attitude 'it will never happen to us'. On the other hand, it is not wise to live in constant fear. We must take a balanced view and a sensible and measured approach to protecting what is important. Whatever we do to protect ourselves, we still cannot be certain that it

will never happen. Even with protection there are no guarantees; there is always a residual risk to contend with. Protecting your car with the latest anti-theft devices does not mean that the vehicle will never be stolen as any protection is never 100 per cent foolproof; there will always be residual weaknesses in the system and, hence, there will always be residual risk. This is true for everything: medicines, IT, food safety, transportation safety, natural disasters, and so on.

Benjamin Franklin once said: 'There are only two things we can be certain of: death and paying taxes.'

So, in essence, risk management activities deal with the uncertainties and how we are able to manage, control and protect our business from the many risks and negative impacts that these uncertainties can cause. There are, of course, certain business activities and operations over which an organization can exercise more control than others, such as internal activities, whereas the organization has less influence, and hence control, over external factors – such as market conditions, the economic and political climate, competition and globalization.

2.1.3 Risk attitudes

A risk to one person might be an opportunity for another person. All humans have a risk attitude: they are risk seekers/risk takers, risk neutral or risk averse to certain things or activities. This attitude can be related to the behaviour of consumers, managers and investors in how they react to uncertainty. Which of these attitudes people adopt depends upon their perception of what is at stake, whether they will win or lose, whether they will be harmed or will be safe, whether they have a fear of taking the risk or they have no problem with taking a chance.

For example, a person is given the choice between two options, one certain and one uncertain. With the uncertain option, the person would need to take a gamble with an equal probability between receiving £100 or nothing. The alternative option is that the person would receive a specific amount of cash with certainty that is a probability of 1:

1. The risk-averse person would accept a certain payment of less than £50 (for example, £40) rather than take a gamble.
2. The risk-neutral person is nonchalant or unconcerned between taking the gamble and a certain £50 payment.
3. The risk-seeking/taking person would be induced to take a certain payment if it is more than £50 (for example, £60) over taking the gamble.

Risk perception is a subjective judgment that people make about the characteristics and severity of a risk and this determines how they react to a risky situation. This subjective judgment means that people will arrive at different estimates and

conclusions of how dangerous a risk is; so it is how they are conditioned and disposed of psychologically to such risky situations. Every time we cross a road or fly in a plane we are taking a risk. Although many millions of people fly each year, some never fly because they are risk averse. Some people gamble with money, others stay away from such activities; it is all a matter of personal choice and conditioning. Each individual will have a different perception of a particular risk situation and so will respond in a different way.

In the business situation risk aversion and risk taking also plays a part. Risk management involves making decisions about risks. If organizations refused to take risks they would not be able to take advantage of the many market opportunities presented to them. On the other hand, organizations cannot be governed by always taking risks on every aspect of their business. Furthermore, those individuals assessing and evaluating the risks and making the decisions may be risk averse or risk takers; it is always important, therefore, to remove any influence or bias towards risk taking or risk aversion. Ideally it is preferable not to work on a single opinion, assessment or evaluation of an individual but to work on the results coming from a team activity.

Of course, trust can play a key factor in influencing perceptions of risk. A business situation is perceived as more risky if the people, or organization, managing the business are perceived as untrustworthy, whereas if the business is being managed by trusted individuals then more credence will be given to this situation than from a management situation that is not trusted.

2.1.4 Pure versus speculative risks

Pure risks relate to loss but not to profit, whereas *speculative risks* relate to a profit or a loss. Most of the risks that businesses take tend to be speculative risks. For example, when the management reach a decision on a business venture or investment based on the chances of success, this could lead to a profit and commercial gain for the organization. On the other hand, the risk of the organization becoming infected with a computer virus, the theft of its commercial information or a denial of service attack represents a potential business loss for the organization. There are some cases where the boundary between the two types of risk is somewhat fuzzy and less straightforward – for example, which political or legal aspects are involved as is the case with data privacy/data protection legislation, legislation and regulations regarding telecommunications systems, or laws relating to forensic evidence.

Risk takers would normally fall into the category of those who are most likely to take speculative risks, unlike those who are risk averse. However, this does not rule out the risk averse being involved in speculative risks: it is a matter of management responsibility and the heuristics used by people to assess the severity and impact of

the risk, whether by 'rules of thumb', educated guesses, intuitive judgments or simply common sense, and should not tend towards irrational risk taking or aversion.

2.1.5 Static versus dynamic risks

Those risks that are always present are referred to as *static* or *generic* risks and include, for example, floods, earthquakes, severe droughts and other natural perils. *Dynamic* risks are those that continue to evolve and change as society changes. They may be driven by economic or political events, new technological developments, social change, legal and regulatory changes and changes to the environment. Static risks are the same as pure risks, but dynamic risks could be speculative or pure. There are some categories of risk that relate to particular business applications, services or systems and so are not necessarily applicable to all organizations or to society at large.

There are some situations in which an organization has more control over the management of the risks, in particular those arising internally, and there are some risks over which the organization has very restricted management influence, such as external risks. An organization can do nothing to influence or control the risk of an earthquake happening, but it can minimize the damage the earthquake might have on its buildings by deploying certain technologies to strengthen the buildings and, therefore, control the extent of the damage.

2.2 Risk factors

There are many types of risk factor within the following categories:

1. Human resources
   a) employment protection
   b) skills and skill shortages
   c) employing people and the employment process
   d) operational deployment of staff
   e) internal versus external staff
2. Legislation, governance and regulation
   a) environment
   b) health and safety
   c) company laws
   d) employment laws
   e) criminal laws

f) data protection and privacy

g) intellectual property and copyright protection

3. Competition and business markets

a) pricing strategies

b) market positioning

c) speculating in new markets

4. Operations

a) business continuity and availability of resources

b) service level requirements

c) maintaining resilient and robust operational facilities

5. Finance and investments

a) returns and profit

b) long- and short-term plans

c) insurance

d) financial regulations

e) legal actions, penalties and liabilities

6. Security and safety

The risks relating to these factors can be rated according to:

1. Impact on business activities and operations

a) downtimes

b) drop in productivity

c) failure to deliver services or a drop in service levels

d) service outage

e) loss in performance

2. Impact on business strategy

a) failure to meet business targets

b) short-, medium- and long-term business effects

c) internal strengths and weaknesses

d) external threats and opportunities

3. Impact on owners/shareholders/company board/company image and reputation
   a) adverse publicity from business or operational failures
   b) drop in shares
   c) legal action

Given the range and diversity of risk factors, taking a formal and structured approach to risk management might be of limited value particularly if the organization does not do business in such a formal and structured way. This is especially the case if speculative risks are always being taken. It is vital, therefore, that any approach taken to implement an effective risk management process is not too rigid, but is as adaptable and flexible as possible to cover a broad strategic view of business risks.

2.3 Corporate risks

2.3.1 Corporate governance

According to the OECD's *Principles of Corporate Governance* [20], good corporate governance '... should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring'. While this directive clearly applies to large, publicly listed companies, it is obviously in the best interests of all businesses that their information risk should be assessed and managed. But, most importantly, effective business process monitoring depends on the effective measurement of information security risk.

While corporate governance can be seen to concern itself, in the main, with the assurance of the rights of shareholders and/or stakeholders within a public company, the corporate governance principles apply to any organization, particularly to those that form part of the supply chain for a public company, and especially if any part of their business is conducted online. The principles concerned are those of disclosure and transparency. An organization's ability to assure all business partners that its information is secured is part of supporting the governance principles of disclosure and transparency.

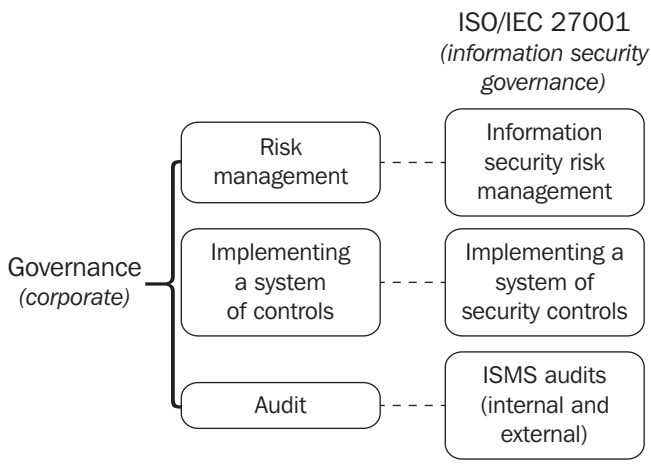
Specifically, the disclosure and transparency principles demand that information is prepared and disclosed in accordance with high quality standards and that channels for disclosure enable unimpeded, easy access to all appropriate information. Moreover, they demand that foreseeable risk factors are disclosed, implying an effectively implemented risk assessment process.

In summary, an organization's effectiveness, corporate governance, operational risk management and the legal and regulatory environment all serve as drivers for the

implementation of an effective ISMS. The ISMS is as important to the operation of an organization as efficient and appropriate information and communications technology systems. Operational risks are risks arising from the execution of a company's business functions. It is a very broad area of risk and includes those relating to fraud, non-compliance with legislation as well as physical and environmental risks. The term 'operational risk' is frequently used in the finance sector, which must organize its risk management programme according to, for example, Basel II under which risk management is divided into credit and market risks, and operational risks. Credit and market risks are normally handled through an organization's financial department, whereas operational risk management is co-ordinated centrally and implemented in different operational units (so the IT department takes care of IT risks, the HR department takes care of personnel risks, and so on).

2.3.2 Information security governance

Information security governance is an essential component of corporate governance. It is a requirement of company directors to demonstrate due diligence in handling information assets on behalf of stakeholders. Information security governance includes all the processes and management decisions that affect company assets in terms of their confidentiality, integrity and availability for business. Without information security governance corporate governance policy cannot be met since there can be little or no assurance and confidence in the internal control system.



Information security governance encompasses all business assets, as well as their risks and threats, including information, processes, people, services, IT and reputation. Thus information security governance involves a risk management

process, which includes IT risks, human resource risks, service risks, and so on. So, from the point of risk, information security governance has a greater scope than IT governance and its line of reporting is directly to the company board of directors and stakeholders.

The organization's policy regarding information security governance should recognize:

1. Information risks are an issue for the board of directors.
2. The accountability for information security risk management lies ultimately with the board of directors.
3. Information security risk management should support and achieve the organization's risk appetite and the approach to integrating risk in management decision-making, providing achievable goals for risk management. The approach taken should meet the needs of the core business activities.
4. Ownership and accountability for managing and reporting information security risks.
5. Roles and responsibilities for managing risk covering:
   a) direct responsibility for the management of risk – e.g. management and staff working within each organizational unit;
   b) responsibility for the development, implementation, maintenance and oversight of the effectiveness of the risk management framework – e.g. a risk committee;
   c) responsibility for providing independent assurance – e.g. internal audit; and
   d) ultimate responsibility for obtaining assurance and thereafter driving improvement. There is a need to take into account how people (e.g. staff) behave or are likely to behave within risk management processes.
6. A well defined and understood policy which sets out the requirements for managing risk and which is effectively communicated across the organization.
7. Well defined processes and procedures for information security risk management.
8. An effective method of assessing and monitoring the organization's information security risk management culture.
9. Clearly defined parameters around the level of information security risk that is acceptable to the organization, and thresholds which trigger escalation, review and approval by an authorized person or body.

10. A well defined approach to recognizing information security risk in management decision-making. Information security risks should be considered in decision-making when any significant business change is planned, be it acquisition of new IT applications, entering into a new area of business, or changing business processes.
11. Specific, timely, accurate and reliable methods of reporting, and an appropriate flow of risk information around the organization.
12. A commonly defined and agreed terminology for key information security risk management principles and practices.

2.4 Organizational risks

2.4.1 General

Organizations are exposed to various types of business risk, which can be categorized in a number of ways. One approach is to consider the source of the risk – examples being investment, legal, operational and market risks. Another is to consider the nature of the asset which is at risk – examples being people, property and information. A further approach is to consider the consequence of a risk in respect of its implications for the long-, medium- and short-term activities of the business – examples being strategic, tactical and operational risks.

An organization will also be exposed to a range of information security risks. These might be recognized as a major category of business risk in their own right or they could be subsumed into other categories, such as strategic and operational risks. An information security risk management system should be capable of dealing with all risks of this kind, irrespective of the way in which they are categorized in business terms.

Information security risk requires the effective control of processes, people and systems, and the monitoring of, and response to, external events. This Handbook aims to give guidance on assessing and managing levels of information security risk. Establishing, implementing and operating, monitoring and reviewing, and maintaining and improving the management system for information security risks is the subject of the related standard, ISO/IEC 27001:2005.

All organizations need to be aware of the need to manage information security risks. Viruses, distributed denial of service attacks, and the potential for system and network compromise could be seen as purely an IT issue. However, the ubiquitous nature of communications and information technologies means that the risks can sometimes turn out to be a complicated mesh of unmanageable interdependencies.

The OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* [19] states the need for '... much greater emphasis on security by governments, businesses, other organizations and individual users who develop, own, provide, manage, service, and use information systems and networks'. This greater emphasis is reflected in worldwide regulatory and legal instruments that place requirements on organizations to improve the management of the confidentiality, availability and integrity of their information throughout the business process. As a result, all businesses that use any form of information processing facilities, such as IT or the internet, have a significant role to play in the management of information security.

Organizations of any size have a number of processes, some of which are internally-facing and others externally-facing. In small organizations there will be limited resources to deal with this work so a number of these processes could be carried out by the same team or even the same person (see also the relationship between roles and responsibilities for organizational processes and assets described in Annex D). As information risk assessment is the responsibility of the whole organization, all parts of a business need to identify the information assets that are critical for their ability to function, and they should ensure that the related risks are assessed and the appropriate security controls are implemented and maintained to manage the identified risks. However, certain risks are specific to certain types of organizational process, and examples of these are described later in this chapter.

2.5 People risk

People-related risks are considered to be the greatest risk facing organizations today, and certainly in the future. These types of risk could be perpetrated by people using IT, deploying operational facilities and processes, or by those having specific organizational privileges and/or management responsibility. People risks can manifest themselves at all levels within the organization. People risks can be internal or external, or both.

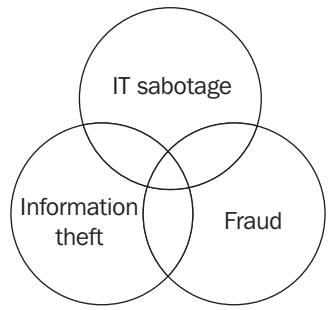
Accidental risks might, for example, be caused by lack of appropriate training or awareness in the use of specific applications, services or systems. They are not motivated by personal gain but are the result of errors, mistakes or making bad judgments or decisions. On the other hand, intentional risks are driven by some motivation, for example, for personal gain, revenge, retribution for unfair dismissal, or the political reasons and views of social activists, terrorists or protestors.

The insider threat is of growing concern as the number of incidents in this area continues to rise. Staff can and do engage in a number of activities that could result in insider threat problems but the three main problem areas are IT sabotage, information theft and fraud.

Examples of fraud, which can be perpetrated by both insiders and outsiders, are:

- financial fraud;
- document fraud;
- identity fraud;
- computer fraud.

An organization needs to give its staff authorization to access and use its information systems in order for staff to do their work and to support the operations of the business. Depending on the type of authorization given, what privileges and access rights are attached to this authorization always leaves open the possibility that staff could exploit this authority to perpetrate harm or damage to the organization's information assets.



Many companies are facing problems with staff morale caused by such factors as downsizing and cost-cutting exercises, the streamlining of business processes, outsourcing of work, problems with the provisioning of staff pensions and many other issues. These problems, together with increases in stress levels, greater workloads and other staff pressures, are causing morale levels to fall which can open the organization up to a range of risks with disgruntled and de-motivated staff, and declining levels of confidence and trust in the organization. All of these issues can lead to some serious information security risks.

Another area relating to the insider threat aspect is that of the 'insider trader' risk. There are both legal and illegal insider trader activities. It is deemed to be illegal where a trader obtains non-public information during the performance of his or her duties within the organization, or otherwise in breach of a fiduciary duty or other relationship of trust and confidence, or where the non-public information was misappropriated from the company. A classic example might be the CEO of a company who learns, prior to a public announcement, that the company is to be taken over and so buys shares in the company knowing full well that the share prices are highly likely to increase in value. In this case the CEO has personally

gained through his or her position in the company and access, at that time, to certain non-public information.

2.6 Operational risk

2.6.1 Risk within the scope of business operations

On the one hand, corporate and strategic risks are concerned with the organization's objectives and where it needs to go, how it plans to achieve these and the direction it needs to take, and how it can ensure its survival. On the other hand, operational risk is the loss of operations resulting from inadequate or failed internal processes, people and systems or from the effects of external events.

The operations of an organization are inextricably linked to the performance of its business and hence to its profit, productivity and ultimate survival in the market. Therefore, any risks to the operating environment and the subsequent impact can have a detrimental effect on business performance. The risks to the operational environment might be as a result of various changes: decreasing product life-cycles, the pace of innovation and the introduction of new technologies, obsolescence, changing economic conditions, commercial exploitation of the internet, staff shortages, lack of skilled staff or low staff morale. Many of the information security risks fall into the broader category of operational risk.

The rigid corporate boundaries that organizations once had are fast disappearing and in many cases their boundaries are more flexible, open, and in some cases almost non-existent. This is as a result of the changing business and economic conditions that have evolved. More organizations are dependent today on third parties as an integral part of their operations to achieve their business objectives and targets. This opening up of organizational boundaries has resulted in more risks being transferred across business and legal boundaries of different organizations and, with the widespread use of the internet, this transfer of risk can now be performed at broadband speeds.

The impact of this is that the organization needs to manage its operational risk outside of the confines of its old corporate boundary but to think in partnership with others to share and support the management of risk. It needs to adopt a flexible and more dynamic risk management approach; the staff and the organization's partners need to understand better how the risks will affect them and their operations, what their collective involvement needs to be and their part in managing the risks within the operational environment.

When a hacker gets into an organization's operational system, the hacker may subsequently be able to connect, using the networks of the organization, to the operational system of one or more of its business partners. This simple scenario

can be expanded to detail other things that the hacker might be able to do having gained access resulting in some very serious security consequences. One immediate consideration is the legal consequences of the hacker having been able to obtain access to the third party operational system using the IT and networking resources of the organization to which the hacker originally gained access.

2.6.2 Externally-facing operational processes

Risks that are specific to particular externally-facing processes are as follows.

1. *Sales and marketing*
   These activities are a vital interface between an organization and the public. In any organization, there is potential risk from failure to protect the confidentiality of sensitive information during sales and marketing operations and of damaging the reputation of the organization through failure to ensure the accuracy and availability of information.
2. *Production and operations*
   Information used by the production and operations processes needs to be highly accurate and consistent, and available when required. The risks of failure should be clearly identified and addressed for those assets that are critical to the production and operations processes.
3. *Customer service*
   This process requires accurate information that is available when required. The consequences of failure are damage to the reputation of the organization, and consequent loss of business.

2.6.3 Internally-facing operational processes

Risks that are specific to particular internally-facing processes are as follows.

1. *Human resources*
   Information security risk is inherent in the interaction between employees and information systems. All employees therefore have a significant role in managing the risk position of the organization. This role must be addressed for recruitment, training, reward, discipline, to termination or change of employment.
2. *Research and development*
   These activities can result in significant risk if there is uncontrolled connectivity between the development and production/operations environments. Research and development can also create very sensitive information, such as that related to products under development. Those involved in such processes should therefore be aware of these risks, and of their responsibility for managing them.

3. *Administration and IT*
   These processes are often regarded as having principal responsibility for the assessment and management of information security risk. However, it is essential that the interrelationship between information risk and organizational risk (see 2.4) is understood and, as a consequence, that information security risk assessment is undertaken by all functions and information security risks are not seen purely as an 'IT problem'.
4. *Finance and accounts*
   Information security risk assessment is of primary importance to the financial and accounting processes of any organization. Good corporate governance (see 2.3.1) requires consistent and accurate financial information that can be traced from its point of origin to its point of use, through a transparent audit trail. The confidentiality of price-sensitive information, undisclosed financial results, and financial forecasts should also be maintained, consistent with business and regulatory requirements.

These are examples of specific information security risks in relation to organizational processes.

All organizational functions need to work together to address organizational risk through the development and use of an integrated and coherent strategy, as described in this Handbook.

2.6.4 Information security and operational risks

In summary, operational risks need to be considered to address the following:

- effects of information security on globalization;
- information security requirements of internal processes;
- information security requirements of processes interfacing with outsourcing and other third party services;
- information security in the deployment of human resources;
- implementation of information security in the use, application and management of IT;
- information security compliance requirements related to current and emerging legislation and regulation.

2.7 IT risk and IT governance

IT itself is not necessarily the security problem. More likely is how the IT is being managed and used. We can, of course, have examples of security problems that are

purely IT-related, such as bugs or faults in software, lack of equipment maintenance, out-of-date upgrades, badly configured IT systems or hardware failures.

However the misuse or abuse of IT systems accounts for a far greater range of information security problems and this brings us back to a 'people' security problem, for example:

- lack of training can cause accidental misuse of IT, user errors and mistakes;
- deliberate use of IT for private use or for personal business, gain and profit;
- sabotage and destruction of IT;
- theft of IT;
- denying availability of resources causing a denial of service.

IT responsibilities as regards IT governance (see ISO/IEC 38500 *Corporate governance of information technology* for further details) include:

- becoming involved in business impact analysis activities with business units and managers;
- preparing proposals for and obtaining approval of risk treatment plans;*
- developing IT structures that implement IT control requirements;
- identifying and analysing threats and vulnerabilities within IT components;*
- keeping up to date with patches, etc;*
- implementing an incident response process;*
- conducting periodic reviews and audits;*
- ensuring that IT security is included during acquisition and development;*
- ensuring awareness regarding information security and user training.*

It is essential that the IT functions and management are in communication:

1. If IT is not in communication with management it will not be able to support business policy and objectives and will not be able to deliver the appropriate IT services and structure.
2. The IT department should understand the business objectives in order to put its IT services in the correct business context and to provide IT support that can protect the organization's information assets.*

The following are some of the expectations for delivery of IT support to the business:

- the IT capability is 'fit for the purpose' of meeting business requirements;
- a flexible IT strategy and structure to adapt to future requirements;

- able to meet business requirements with regard to throughput, response times, capacity, availability and performance;
- ease of use;
- robust and resilient;
- security of information and IT.*

*Note: * indicates that these objectives can be achieved by adopting ISO/IEC 27001:2005.*

There are several IT measures that may be used by a business to assess the success of its IT governance:

1. Increase in revenue
2. Return on IT investment
3. IT products:
   a) time to bring a new product to the market and sales from new products
   b) product quality
4. Services:
   a) level of service quality and delivery
   b) customer satisfaction
   c) delivery of IT value per customer/employee
5. Infrastructure availability
6. Cost of transactions
7. Partnering success
8. IT skills and competence